HTTPS最佳实践

自信地部署HTTPS

耗费最少的时间，达到最佳的效果

MySSL.com

HTTPS 最佳实践

SSL/TLS最佳实践

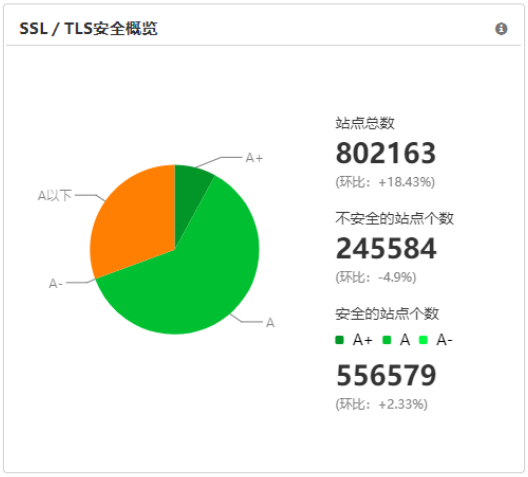
自信地部署SSL
耗费最少的时间，达到最佳的效果

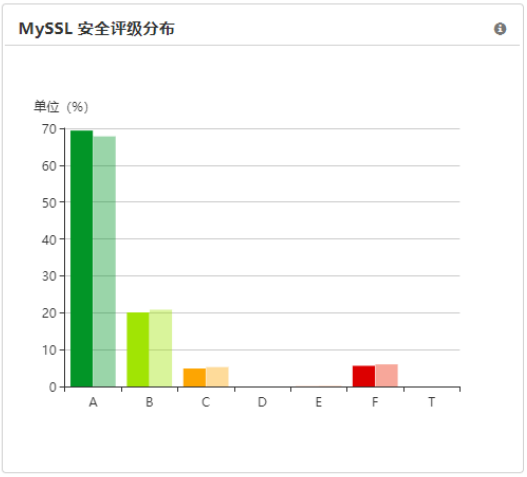
MySSL.com

一、 简介

HTTPS 所使用的 SSL/TLS 协议作为一种互联网安全加密技术，在实现安全性的同时也伴随着许多风险。例如，可以针对 SSL / TLS 协议制定攻击；服务器供应商、认证机构（CA）不合理设计的协议也给攻击留下了可乘之机；又或者你可能在服务器上错误的执行 SSL / TLS，这也会增加被攻击的风险。

MySSL.com 为广大网站运营商和用户提供了在线检测工具。迄今为止，已有 802163 个站点使用 MySSL.com 对站点进行检测评级，近三分之一的站点评级为不安全。





这些评级为不安全的站点有的支持 SSL 2.0 和 SSL 3.0，有的使用不安全的密码套件，又或者支持 RC4 等弱密钥。

评级不佳的网站存在的问题不是因为系统缺陷，而是由于不合理的配置和部署。

SSL / TLS 看似简单，似乎很容易部署，但事实并非如此。

MySSL.com 已经全方位地审查了 SSL / TLS 部署过程，为您提供最佳实践，使您可以在部署和维护上花费最少的时间，达到最佳的效果。

SSL/TLS 部署最佳实践

本书目标是为您提供 SSL/TLS 部署最佳实践秘诀，专业的部署知识，同时鼓励您采用 Always-On SSL 方法，并建议您从可靠的 CA 获取证书。

SSL / TLS 最佳实践详细说明了在部署 SSL / TLS 时应当正确部署并定期监视和维护的所有内容：

- 私钥和证书；私钥保护，密钥大小和签名算法。
- 服务器配置；有效证书链，安全协议，安全密码套件，重协商和压缩。
- 应用程序保护；恶意软件，SQL 注入，跨域脚本攻击（XSS），混合内容（Mixed content），第三方信任，安全 Cookies。
- 增强服务器安全性；优先正向保密（Perfect Forward Secrecy），OCSP 装订（Stapling）和 HTTP 严格传输安全（HSTS）。
- 域保护；认证机构授权（CAA），证书透明度（Certificate Transparency），公钥固定（Key Pinning）以及证书声誉(Certificate Reputation)。
- 高级证书；EV 证书，多域名证书和私人可信（Private Trust）证书。
- Always-on SSL；保护网站免于常见的攻击（例如，MITM，SSLstrip 和 Firesheep）,提供安全性和保密性。

注意：除以上注意事项，我们还建议您在部署 SSL / TLS 时，应选择一个可靠的 CA 来获取证书。可靠的 CA 可以提供证书管理，证书发现和响应式 CRL 以及 OCSP 响应，提供各种证书类型和灵活的验证模式。 还具有很好的技术支持，包括服务器安装，服务器证书和网站扫描。

二、 证书和私钥

当提及网络安全的时候，身份和身份验证是非常重要的。证书是安全领域的身份证，可以有效解决网络世界中“你是谁”的问题。私钥用于身份验证，就像一把钥匙一样，两者协同工作，以确保您网站的最大安全性。

下面介绍证书和私钥的具体内容，遵循这些步骤，确保您网站安全性始终处于领先地位。

私钥保护

为了确保网站的最大安全性，必须确保服务器私钥处于保护状态，而且必须定期更换。

为防止网站被攻击，服务器应始终具有物理和逻辑保护。每个私钥也应该加密并备份存储。

在某些情况下，例如，对于用于保护高敏感数据和应用程序的受信任密钥，应考虑密钥的硬件保护。

重新颁发证书时，应生成新密钥。这将确保密钥的旧副本不再起作用。在发现威胁甚至是可疑的安全漏洞之后，请确保生成新密钥并撤销旧证书。

密钥大小

对于期望保持机密性至 2030 年的数据来说，加密密钥的大小为 2048 位 RSA 密钥是目前为止推荐的最佳值。

我们通过增加密钥大小来缓解针对私钥的攻击，但密钥大小的增加会降低服务器的性能。ECC 密钥解决了这一问题，它提供小尺寸密钥，同时也确保了强大安全性。256 位的 ECC 密钥的安全强度大于 2048 位 RSA 密钥，服务器现在开始支持 ECDSA 密钥，并且大部分的浏览器软件也都支持 ECC。下图为 RSA 与

ECC 密钥安全性的比较：

攻破时间	RSA/DSA	ECC密钥长度	RSA/ECC
MIPS年	密钥长度		密钥长度比
10^4	512	106	5:1
10^8	768	132	6:1
10^{11}	1024	160	7:1
10^{20}	2048	210	10:1
10^{78}	21000	600	35:1

MIPS(Million Instructions Per Second)，每秒处理的百万级的机器语言指令数。这是衡量 CPU 速度的一个指标。

使用较大的密钥并不会带来更多的好处，因为它会降低服务器性能。如果您计划在多台服务器上安装证书，请考虑使用具有不同密钥的证书。这样，如果一个密钥被泄露，那么只有相应的服务器将受到损害，其他的不会受到影响。

签名算法

所有服务器和应用程序都必须支持或迁移到支持 SHA-2 算法。

微软和谷歌已弃用了 SHA-1 算法，这意味着仍然使用该标准的网站将在他们的浏览器中被视为不值得信赖的网站。使用 SHA-1 算法的证书已经在 Chrome 中显示错误。

2017 年，Windows 不再支持 SHA-1 签名的证书。迁移到 SHA-2 要求中间证书也要用 SHA-2 签名。大多数 CA 将支持 SHA-2 并使用 SHA-256 版本的散列算法。

证书有效期

对于 OV 和 EV 证书来说，最长有效期为 39 个月， EV 证书的最长有效期为 27 个月。证书有效期越短越有助于保护您的私钥。 如果您的证书有效期降至一年，则可以每年更新密钥，可能遭受攻击的时间也会减少。

6 个月或 3 个月怎么样？ 您的 CA 应该支持您选择适合您的应用程序的证书有效期。

证书吊销状态

浏览器如何检查证书吊销状态？

工具	定义	优点	缺点
证书吊销列表（CRL）	CA 证书签名的所有已撤销证书的序列号的签名列表	CA 证书颁发的所有证书状态的单一参考点。	随着时间的推移，CRL 可能会非常大，导致不可接受的延迟。攻击者可能会利用此延迟阻塞 CRL 信息的传达。
在线证书状态协议（OCSP）	包含一个证书状态的签名响应。	OCSP 响应很小，不会增长。 因此，不会因大小而发生延迟情况。	浏览器必须获取 Web 服务器证书链中的每个证书的 OCSP 响应，这就要求服务器打开额外的连接，会影响页面加载速度。隐私问题可能是需要关心的，因为 CA 可以决定用户访问哪些网站。攻击者可能会阻止 OCSP 发送消息。
OCSP 装订（Stapling）	由 Web 服务器实现缓存的签名响应，包含证书的状态。Web 服务器将 OCSP 响应发送给浏览器。	没有隐私问题，因为 CA 不知道哪个用户请求 OCSP 响应。	需要支持 OCSP Stapling 的 Web 服务器和浏览器。攻击者可能会阻止 OCSP 发送消息。
Blacklist（例如 CTLS 或者 CRLSets）	由浏览器供应商分发的证书列表，不应该被信任（不管它们是否被撤销）。	黑名单由浏览器供应商分发，作为浏览器可执行文件的一部分。黑名单上任何证书都可以被拒绝，无需任何额外的检查。	出于实际原因，该清单不完整。

软故障与硬故障（Soft-fail vs. Hard-fail）

浏览器用户主要关注的是软故障与硬故障策略。证书颁发机构（CA）CRL/在线证书状态协议（OCSP）响应可能无法传递给浏览器，这可能是由于基础架构中某处出现非恶意故障而导致的，但也可能是因为遭受攻击而发生的。

浏览器设计者已经确定前者的解释可能性非常大，因此他们选择了软故障策略。这意味着如果浏览器没有收到任何响应，那么证书将被认为是可信的，浏览器将允许访问相关内容。

另一方面，硬故障策略意味着如果浏览器没有收到响应，则假定证书被撤销，浏览器将阻止访问内容。

在撰写本文时，没有主要的浏览器采取硬故障策略。

最佳做法是与 CA 合作，CA 以可靠的方式提供 CRL 和 OCSP 响应。及时响应并帮助所有用户通过 HTTPS 安全地快速访问您的站点。

在后面的章节中我们将讨论 OCSP Stampling 和 OCSP Must-Staple。

域名覆盖范围

为了保证最大的覆盖范围，请确保域名的 www 和没有 www 都解析为同一个 Web 服务器并受 SSL 保护。

您永远不知道用户将如何访问您的网站; 因此，确保 www.example.com 和 example.com 都被重新覆盖至关重要。

虽然这两个标准对用户来说没有功能上的差异，但我们发现更多的用户在访问网站时喜欢使用没有 www 的域名。

自签证书

我们不建议网站使用自签证书。

自签证书是由认证自己身份的同一实体签名的身份证书。换句话说，除了网站所有者之外，其他任何人都不能对其进行验证。这意味着用户必须相信所有者是他们所声称的人，自签证书不保证遵循正确的安全程序。

自签名证书遵循的是所有者自定策略，可能不遵循行业准则或最佳实践，并且未经过审计。

自签名证书在浏览器中不会获得与 CA 签名证书相同的信任，并且容易包含

过期证书。

自签名证书模型

- 证书所有者自证
- 所有者依据自己的政策发布证书
- 所有者对证书质量负责
- 所有者可能不遵循行业准则
- 所有者可能不提供证书状态
- 受损的证书可能不能够撤销
- 所有者未被审计
- 证书颁发者可能未经域名所有者授权
- 如果没有提示，证书可能不会被更新
- 自签名证书模型不被信任，浏览器提示不可信

由 CA 签名的受大众信任的证书模型

- CA 验证域名所有者和证书申请者
- CA 按照浏览器和操作系统供应商的要求制定政策。这些要求包括 CA/浏览器论坛基线需求（CA/Browser Forum Baseline Requirements）、扩展验证（EV）指南和 NIST 的建议
- CA 提供质量保证。实施证书检查，确保不使用受损的密钥，遵循指导原则，确保使用的密钥不低于最小值，以及合理的散列算法、最大有效期和合理的

证书扩展。

- CA 基于行业最佳实践更新策略
- CA 通过 CRL 和 OCSP 提供证书状态
- 受损的证书会被撤销
- 根据证书颁发标准对 CA 进行审核，例如 WebTrust for CA，WebTrust for EV 和 SSL Baseline Requirements 等标准。
- 域名验证（DV）证书的证书请求者是由域名所有者授权的。组织和扩展验证（OV 和 EV）证书的请求者是由证书中指定的组织成员授权的。
- CA 提供多次提醒，以确保证书在过期之前更新。CA 还可以提供证书发现工具，以便在您的系统上找到可能没有提醒的即将过期的证书。
- CA 模型作为受大众信任的模型，主要是因为 CA 对于浏览器/OS 供应商，网站证书订阅者和网站最终用户是值得信任的第三方。CA 有义务满足所有三方的要求。

最佳实践是使用由可靠 CA 颁发的 SSL/TLS 证书。

三、 服务器配置

正确的配置您的服务器是保证服务器安全性的最佳方法之一。虽然 SSL/TLS 是一个可靠的标准，但是不正确的配置会产生危及安全性的漏洞。

下面的部分概述了一些主要的工具和解决方案，这些工具和解决方案可以用来确保您的服务器被正确配置，并且避免任何潜在的漏洞。

有效证书链

SSL 证书必须由发行 CA 发布（也称中级或下级 CA），而发行 CA 可能是根 CA 下的一层或多层。因此，在安装 SSL 证书时，您必须安装所有的发行 CA 证书。

安装了所有的发行证书之后，根目录下就会生成一个有效的信任链。

MySSL.com 在线检测 myssl.com，检测报告给出的证书链信息如下图：

随着时间的推移，您可能必须更新您的发行 CA 证书。例如，发行 CA 证书应该总是比 SSL 证书的有效期更长。在加密算法更新的情况下，如从 SHA-1 更新到 SHA-2，您还需要安装一个 SHA-2 发行 CA 证书。

注意：您不需要安装根证书。因为浏览器已经有一系列可信的根证书。加入另一个根证书只会使您的 SSL 握手时间延长，从而使安全会话的建立时间变长。

安全协议

在过去的 20 年里，SSL/TLS 协议已经发展成为一个安全行业标准。然而，一些重要的变化已经出现。

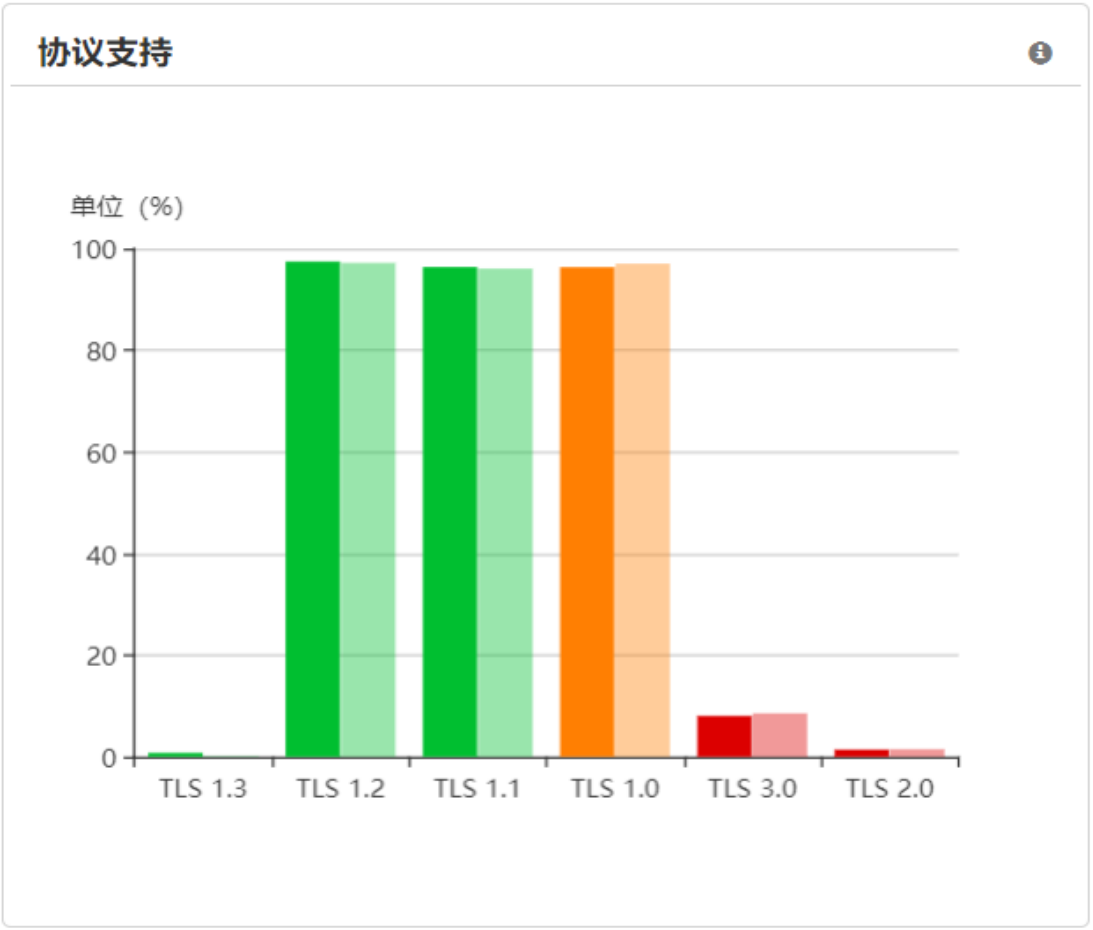
SSL 2.0 和 SSL 3.0 不应该再被使用。

携有 POODLE 漏洞的 SSL 3.0 的新问题引起了人们的注意，所以目前浏览器不支持 SSL 3.0。

在部署 SSL/TLS 时，请确保实现 TLS 1.0 和 1.1 的向后兼容性。TLS 1.2 也应该实现向后兼容性，它不存在任何已知的安全问题。

注意：TLS 1.0、1.1 和 1.2 的一些实现很容易受到 POODLE 的攻击，为了缓解攻击应当定期实施升级。

MySSL.com 会每月生成“HTTPS 安全报告（月报）”，该报告能展现目前国内网站的协议支持情况。



安全密码套件

SSL/TLS 协议使用密码套件保护通信中的数据。密码套件都倾向于使用较长的描述名称，并且相当一致：它们都是由密钥交换方法、身份验证方法、密码定义以及可选的 MAC 或 PRF 算法组合而成，如下图所示：

服务器上配置了许多密码套件，以支持所有与服务器交互的的浏览器或应用程序。随着时间的推移，密码套件中的一些算法可能会变得不安全。密码套件应该使用最小 128 位来进行身份验证和加密。

RC4 加密算法不应该被使用，因为它容易受到攻击，并且不被浏览器信任。

为了减轻异常，服务器管理员应该禁用对任何导出 RSA 套件的支持。

注意：为了缓解 Logjam 漏洞，建议服务器管理员禁用对包括 DHE_EXPORT 在内的所有导出密码套件的支持。 同时鼓励管理员使用 1024 位 DHE 新生成的密码套件，或者部署 ECDHE 作为替代方案。

下图为 MySSL.com 根据检测到的（中国）站点客观数据统计出的站点加密套件强度分布情况：

重协商

重协商允许服务器和浏览器停止交换数据，以便重协商新的 SSL/TLS 握手。不需要客户端启动重协商，如果启用，则可能会产生 Dos（denial of service，DoS）攻击的机会。

由于不安全的重协商，新旧 TLS 流之间没有连续性。

因此，重协商的握手可以通过不同的客户端浏览器来完成。服务器应该能够被配置以进行安全的重新协商。如果没有安全的重协商，那么就应该取消重协商。

TLS 压缩

CRIME 攻击表明，由于 TLS 压缩导致的信息泄漏可以用于发现敏感数据。**服务器上应该禁用 TLS 压缩。**

HTTP 压缩

TIME 和 BREACH 攻击揭示了 HTTP 压缩存在的问题。HTTPS 压缩是非常有用的，所以删除不是一个实际的选择。由于攻击很难实现，因此不建议服务器更改。

TIME 和 BREACH 攻击只会使 SSL 3.0 和 TLS 1.0 变得脆弱，因此当我们支持 TLS 1.1 和 1.2 或更高版本时，受攻击概率将会降低。

四、 应用程序保护

一旦配置了服务器，您就需要确保应用程序是安全的和受保护的。考虑将应用程序保护作为保障网站安全的方法。

您需要确保在服务器上运行的应用程序是安全的。它不能运行恶意软件，也不应该遭受常见的攻击，比如跨站脚本（XSS）或 SQL 注入（SQLi）。

在某些情况下，在实现应用程序保护的同时，您可能会发现您的网站已被搜索引擎列入黑名单。在其他情况下，网站可能有混合的 HTTP 和 HTTPS 内容，或者没有使用安全 Cookie。

这些错误都可以通过站点扫描检测到，使您可以实现应用程序保护。

建议：使用可信的分层网站安全性。

为什么分层网站安全？

- 使用 SSL 加密来保护网站和身份
- 发现并移除恶意软件
- 域名黑名单
- 消除网站漏洞
- 删除网络弱点

恶意软件

每年有超过 50 亿次恶意软件攻击事件的发生。

恶意软件通过恶意的 JavaScript 注入网站。一个典型的网站可能有成百上千的潜在的漏洞可被利用以注入恶意软件，这些漏洞不容易被检测到。

一旦恶意软件注入到网站，它就会传播病毒，窃取个人或财务信息，劫持电脑或感染你客户的电脑（在客户访问你的网站后）。最终，这将对网站的声誉造成负面影响，并可能导致业务流失。

针对恶意软件，应当每天对网站实施扫描。

如果搜索引擎在网站上发现恶意软件，网站会被列入黑名单，那么搭建网站所有的努力与投资都将白费。如果你的网站直接或间接地链接到被列入黑名单的第三方网站，那么你的网站也可能被列入黑名单。

应该每天监控黑名单，以确保你的网站不会出现在列表中。

SQL 注入

SQL 查询可能会受到攻击者的操控。攻击者可以将恶意 SQL 语句输入到可以执行的查询中。

我们将其称为 SQL 注入（SQLi）。通过注入 SQL 语句攻击者可以访问存储在数据库中的敏感信息。

应该每天对站点进行扫描，以确定它们是否容易受到 SQL 注入技术的攻击。

跨站点脚本攻击(XSS)

跨站点脚本（XSS）主要有两种类型：Reflected 和 Stored。

当攻击者创建的脚本或编码是通过第三方工具（比如电子邮件）发送的，Reflected 或 Non-persistent 的 XSS 攻击就会发生。

在电子邮件中发送一个脚本，要求受害者点击一个链接，验证他或她的登录信息，或者使他访问一个特定的网站。当受害者点击链接时，代码将被发送到 Web 应用程序，然后返回给受害者，恶意代码或脚本就会执行。

受害者输入的任何信息都可以发送给黑客，Session Cookie 可能被窃取。

当脚本或恶意软件直接存储在 Web 应用程序中时，就会发生 Stored 或 Persistent 的 XSS 攻击。

Stored 的 XSS 攻击是最具破坏性的，因为它们会影响到特定页面或链接的所有访问者。

开放 Web 应用程序安全项目（OWASP）提供了避免 XSS 攻击的方法。

应该对站点每天进行扫描，以确定是否存在跨站点脚本漏洞。

过时且易受攻击的应用程序

随着时间的推移，应用程序可能会变得容易受到代码缺陷，过时版本和过时策略的影响。随着应用程序的老化，攻击者将会找到方法来破坏这些程序。这类型攻击的影响是广泛的，并且很大程度上取决于被攻击的应用程序的类型。

应用程序漏洞可能是:

- SSL / TLS 协商 DoS
- HTML 注入
- 跨站脚本攻击（XSS）
- SSH 服务器类型和脚本
- Robot.txt 文件
- ICMP 时间戳请求远程日期披露
- Cookie 注入
- SQL 注入（SQLi）
- Web 服务器 info.php /phpinfo.php 脚本检测

网站所有者应该考虑每天扫描他们的应用程序，以寻找常见的漏洞和未修补的软件。

混合内容（不安全外链）

如果 HTTPS 页面包含通过常规的明文 HTTP 获取的内容，那么这种连接只会部分加密。

未加密的内容可以被嗅探器访问，并且可以通过中间人攻击被更改。

从其他站点获取的所有内容都必须进行加密，以减轻混合内容的脆弱性。

第三方信任

如果您使用的第三方服务是通过 JavaScript 从另一个服务器激活的，那么，从本质上说，您必须信任第三方。如果第三方受到攻击或疏忽，那么你的网站可能会受到攻击。

请考虑您的第三方服务的来源，并确保您在实施之前信任第三方。

安全 Cookie

不安全的 Cookie 会受到中间人攻击。

服务器应该始终使用安全 Cookie。

五、 服务器增强安全性

增强服务器安全性对于保护您的网站免受最具破坏性的攻击、他人利用和其他安全威胁至关重要。

通过部署诸如优先正向保密（Perfect Forward Security）、OCSP 装订（Stapling）、ECDSA 私钥、HTTP 严格传输安全（HSTS）和 HTTP/2 等技术，您可以提高服务器性能并确保您的网站始终受到保护。

若想确认您的网站是否部署了可以增强服务器安全性的技术，在 MySSL.com 中输入您的网站，检测报告的协议详情部分为您提供了详细的部署信息。如下图所示：

协议详情

HTTP/2	支持	
新型的TLS配置	是	
支持TLS 1.3（draft 28）	不支持	
期望CT	不支持	
OCSP装订	不支持	
预防降级攻击	支持	
正向保密	支持	
HTTP严格传输安全(HSTS)	支持	max-age=15768000; includeSubDomains; preload
公钥固定(HPKP)	不支持	
公钥固定报告	不支持	
XSS保护	支持	1
CAA	不支持	
NPN	支持	h2,http/1.1
ALPN	支持	h2,http/1.1
TLS心跳(扩展)	不支持	
支持的EC椭圆曲线	支持	secp256r1
SSL2握手兼容	支持	
会话恢复(caching)	支持	
会话恢复(Ticket)	支持	
STARTTLS	不支持	
过长的ClientHello兼容	不支持	
未知TLS版本兼容	不支持	
不正确的SNI警告	不支持	
DH公钥参数重用	否	不支持DHE系列的加密套件
ECDH公钥参数重用	否	
服务端安全重协商	支持	
客户端安全重协商	不支持	
客户端不安全重协商	不支持	
支持RC4套件	不支持	
是否为邮件服务器	否	

优先正向保密

优先正向保密（Perfect Forward Secrecy ,PFS）确保服务器的私钥和每个会话密钥之间没有关联。

如果客户端和服务器都支持 PFS，他们就会使用一种名为 Diffie-Hellman 的协议变体，在这个协议中，双方都安全地交换随机数，并达成相同的共享秘密。这是一种聪明的算法，可以防止窃听者获得相同的秘密，即使窃听者可以查看所有的数据流。

当使用包含 RSA 的 ECDHE 密码套件和椭圆曲线加密（ECC）SSL 证书时，

所有浏览器都支持 PFS。除了 IE 之外，所有的浏览器都支持使用包含 RSA 的 DHE 密码套件的证书。

您还可以测试您的浏览器，看看它是否支持 PFS。如果您的网站需要支持旧浏览器，而旧浏览器可能不支持 PFS，您将不得不配置您的 Web 服务器来提供非 PFS 套件。

PFS 的实施将有助于避免监控(Pervasive Surveillance)的威胁。

在线证书状态协议（OCSP）装订

数字证书状态由证书撤销列表（CRL）和在线证书状态协议（OCSP）提供。

CRL 是所有已吊销证书的列表。如果一个证书的序列号不在 CRL 列表中，则认为该证书是正常的。OCSP 为所有证书提供响应。简单来说，无非两种状态，要么正常，要么不正常。

关于哪一种方法最有价值，这要归结到证书颁发机构 (CA) 和用户站点访问方式。如果 CA 吊销了大量证书, 管理了大量的 CRL, 则不推荐使用 CRL, 因为 CRL 过大，需要花费很长时间才能下载。

在移动设备上, 用户可能不想下载大文件, 也可能没有存储文件的空间。因此, 在移动世界中, OCSP 是最受青睐的方法。

OCSP 响应可以通过两种方式提供：

1. 最常见的方法是 CA 操作 OCSP 服务。当浏览器要获取证书的状态时, 它会从证书的扩展名中找到 OCSP 服务器, 检查证书是好还是坏。此方法需要浏览器依赖 CA 提供的服务。不幸的是, 有些 CA 不擅长提供 OCSP 响应。在某些情况下, 没有服务；在其他情况下, 服务太慢了。服务过慢意味着它尝试加载的网站上产生了延迟。

2. 第二种选择是 OCSP 装订。在 OCSP 装订中, WEB 服务器从 CA 获得 OCSP 响应。当浏览器访问站点时, OCSP 响应将被装订在 SSL 握手中。这意味着与 CA 的 OCSP 服务器没有额外的连接。这将带来更少的延迟时间和更快的网站加载速度。它还允许网站所有者通过增加服务器的吞吐量来管理自己的性能, 他们的网站会变得更受欢迎。对于 CA 也是有好处, 它不必为高度活跃的网站提供额外的性能补偿。

如果您正在运行一个网站并希望减少延迟, 请考虑实施 OCSP 装订。您需

要了解服务器是否支持装订。例如，Apache 2.3.6+，Microsoft IIS 7+（默认情况下启用装订）和 Nginx 1.3.7+都支持 OCSP 装订。

OCSP Must-Staple

OCSP Must-Staple 解决方案可以帮助解决 CA 的 OSCP 服务器问题。如果 WEB 服务器可以安全地告知浏览器它支持 OSCP 装订，那么浏览器就会知道需要一个 OSCP 装订响应。如果没有收到响应，浏览器可能会实施硬故障。

网站管理员必须决定他们的网站是否需要支持 OCSP Must-Staple。首先，他们将不得不使自己的网站支持 OCSP 装订，然后他们必须添加 OCSP Must-Staple 标志。设计并未最终完成，OCSP Must-Staple 标志可以通过两种方式实现:

1. SSL 证书中声明 Must-Staple

在这种情况下，网站管理员必须通知它的 CA，它需要 OCSP Must-Staple。CA 将在 SSL 证书中放置一个对象标识符 (OID) 扩展名，标明 Must-Staple。当用户访问该网站时，浏览器将检查该证书并查看 OCSP Must-Staple 标志。然后，它将需要来自 WEB 服务器的 OCSP 装订响应。如果没有收到响应，则浏览器实施硬故障。

2. SSL 响应头中声明 Must-Staple

对于 OCSP Must-Staple 更直接的解决方案是将该标志包括在 HTTP 响应头中。Mozilla 开发者目前正在研究这个解决方案。

在这种情况下，Web 管理员将在其 Web 服务器响应中添加一个 Must-Staple 响应头。该响应头将包括一个时效说明，它将告诉浏览器 Must-Staple 标志在一定的时间内有效。浏览器将缓存 Must-Staple 信息。

下次浏览器进入网站时，它会知道这是一个 Must-Staple 的网站。如果没有收到 OCSP 装订，则浏览器实施硬故障。

这个解决方案存在一个 "初次访问" 的问题。即除非浏览器访问过站点，否则它将没有 Must-Staple 信息。这就允许攻击者在浏览器首次访问网站时实施干扰。解决方案虽然好但并不完美。通过预加载的 Must-Staple 站点列表可能能够减轻攻击。

以下是 OCSP Must-Staple 的概况:

实现方式	定义	好处	坏处
OCSP Must-Staple（证书中声明）	该标志是在 SSL 证书中作为特定对象标识符 (OID) 扩展实现的。	没有 "初次访问" 问题，与 Web 服务器的所有连接都带有 Must-Staple 标记。	Web 服务器需要使用附有 OCSP Must-Staple 标志的证书。
OCSP Must-Staple(HTTP 响应中声明)	该标志作为 HTTP 响应头实现	使用现有的 SSL 证书。	“初次访问”问题

OCSP Must-Staple 解决了传统的吊销检查存在的大多数问题，允许浏览器实施硬故障策略。尽管仍存在一些缺点，但都是部署浏览器和 WEB 服务器支持 OCSP 装订和 Must-Staple 需要解决的问题。

目前，所有新的桌面浏览器都支持 OCSP 装订。对于 WEB 服务器，Microsoft IIS 默认支持 OCSP 装订，Apache 和 Nginx 的所有版本可以配置为支持 OCSP 装订。其他服务器 (如 F5) 也将很快支持 OCSP 装订。

椭圆曲线 DSA（ECDSA）私钥

几乎所有服务器都使用 RSA 密钥。我们通过增加密钥大小来缓解针对私钥的攻击。例如，我们已经从 1024 位转移到 2048 位。但是，密钥大小的增加会降低服务器的性能。

椭圆曲线加密算法解决了这一问题，它提供小尺寸密钥，同时也确保了强大安全性。因此，服务器现在开始支持 ECDSA 密钥。并且大部分的浏览器软件也都支持 ECC。

在短期内，如果要部署 ECDSA，您还需要支持 RSA 密钥以确保向后兼容性。某些服务器将允许您同时拥有 RSA 和 ECDSA 密钥。这有利于将来移除 RSA。

HTTP 严格传输安全（HSTS）

HTTP 严格传输安全 (HSTS) 是一个非常好地保护您网站的方法。HSTS 的实现是 Always-On SSL 策略的扩展。

对于您希望使用 HSTS 进行保护的网站，首先必须要部署 SSL/TLS 证书(如果尚未部署)，配置网站为仅通过 HTTPS 访问，不允许通过 HTTP 访问。然后，您通过发送 HSTS header，向启用了 HSTS 的浏览器传达您的站点只能使用 HTTPS。支持 HSTS 的浏览器将自动把发向某网站的所有 HTTP 请求更改为 HTTPS 请求。

如果没有可用的 HTTPS 版本，则浏览器将向用户提供信任对话框。

HSTS 在 IETF RFC 6797 中定义，并且正在被大多数浏览器部署。不支持 HSTS 的浏览器将忽略 HSTS header，因此网站管理员无需等待所有浏览器支持。

减轻的风险

HSTS 有助于阻止基于 SSLstrip 的中间人攻击，SSLstrip 能够将 HTTPS 的域请求更改为一个类似站点 HTTP 的域请求。如果使用 HSTS，浏览器将能够检测到从 HTTPS 到 HTTP 的域名更改。

HSTS 还将缓解以下安全问题:

- 用户设置书签或手动键入的 HTTP 域请求将被重定向到的 HTTPS 的目标域请求。
- 无意中包含 HTTP 链接的 HTTPS 站点将被重定向为 HTTPS 的目标域请求。
- 如果中间人攻击将用户重定向到无效证书，HSTS 将不允许用户覆盖无效的证书消息。

即使您的网站不托管或请求任何敏感数据，但使用全站 HTTPS 能为你的站点提供一致的外观与感受，同时确保用户通信安全。

支持

Chrome，Firefox，Opera 和 Safari 均支持 HSTS。2015 年发布的 Windows 10 也支持 HSTS。对于浏览器是否支持 HSTS，可以通过 "Can I use Strict Transport Security?"检查。

HTTPS 重定向怎么办？

大多数网站管理员都非常熟悉重定向，他们通常建议使用技术强制将连接从 HTTP 转到 HTTPS，作为 HSTS 的替代方法。

不幸的是，重定向需要通过 HTTP 与服务器进行初始连接，这是易受攻击的。

当浏览器与站点进行初始连接时，攻击者可以获得不安全的会话 Cookie，还可以在未加密响应中注入恶意内容 (如假的登录页面)。如果浏览器知道站点通过 HSTS 请求 HTTPS，它将比简单的重定向更安全。

HTTP/2

HTTP/2 是 Web 使用的网络协议的下一个主要版本。

HTTP/2 以 Google 的 SPDY 为基础开发，并已在 Chrome、Firefox、Opera、Safari 和其他浏览器上实现。HTTP/2 的目标是允许客户端/服务器选择一个协议，并保持与 HTTP /1.1 的兼容性，降低页面加载延迟，支持 HTTP 的常规现有用法。

Google 和 Mozilla 开发团队都已经宣布他们打算仅通过 TLS 支持 HTTP/2。其他浏览器都将效仿，使该标准成为强制性的。因此，要获得 HTTP/2 的最大好处，必须部署 TLS 。

服务器名称指示（SNI）

当您想继续部署 Web 服务但 IPV4 地址耗尽时，可能会出现两难境地。您考虑部署使用相同 IP 地址的多个虚拟服务，但是，您的想法是每个 IP 地址只能有一个 SSL 证书。您将如何确保您的服务安全性呢？

服务器名称指示 (SNI) 是 SSL/TLS 协议的扩展，允许浏览器或客户端软件指示它试图连接的主机名。SNI 是在 RFC 6066 中定义的。

通过在服务器上支持 SNI，您可以提供多个证书并在同一 IP 地址支持多个服务器。客户端指示主机名，服务器选择正确的证书来完成 SSL 握手过程。

为了使 SNI 有效，它必须被大多数浏览器实现，幸好现在就是这种情况。如果浏览器不支持 SNI，则将显示默认证书。如果证书不支持请求的域名，则会看到证书警告。当然，如果证书是支持请求的子域的通配符证书，则不会出现警告。

SNI 可以在发生中间人攻击时中止连接。例如，如果浏览器请求连接到特定域名的服务器，但收到的证书不支持该域名，则会出现一个证书警告，这表明可能受到了中间人（MITM ）攻击。

SNI 可以使用多张证书或一张证书进行部署。多张证书仅仅意味着一个证书支持一个域名。或者，您可能希望将相关站点组合在一起使用一个证书；例如,通配符或多域名证书。多域名证书允许将多个域名添加到备用名称(SAN)字段中，

只是因为证书的大小，会付出降低性能的代价。随着更多的域名被添加，多域名证书须被即时更新, 或选择添加新证书。

缺点是并非所有的客户端 (如 Windows XP) 都支持 SNI。因此, 在 XP 上运行的 IE 浏览器将无法正常工作, 尽管 Windows XP 不再被官方支持, 但 Microsoft 确实为乐意支付的企业提供了特殊的长期支持。替代浏览器将帮助缓解 XP 问题, 因为 Chrome, Firefox 和 Opera 都将在 XP 上支持 SNI。

支持较少 IP 地址的安全性的替代方法不是部署 SNI, 而是使用单个多域名证书。如果域名由不同的实体拥有或控制, 则此解决方案会受到限制。每次需要支持新域时，都必须更新多域名证书，所以可能还存在证书管理的问题。

SNI 的优点是可伸缩性。SNI 将允许您使用较少的 IP 地址和较少的服务器部署 SSL。它将允许独一无二的证书用于不同的网站, 身份和品牌, 这可以提高安全性和信任度。Windows XP 用户在逐渐减少, SNI 将是支持较少 IP 地址多域名的最佳选择。

六、 域名保护

许多 CA 可以为您的域名颁发证书。有一些方法可以保护或监控您的域名证书，确保您的安全，免受错误实现或攻击的影响。

- 证书颁发机构授权（CAA）
- 证书透明度（CT）
- 证书声誉
- 公钥固定

证书颁发机构授权(CAA)

拥有众多公共 CA 存在的一个问题是，任何一个 CA 都可以为任何域名颁发 SSL 证书。对于那些审查了 SSL 行业然后选择了一个他们可以信任并与之合作的 CA 的用户来说，这将是令人沮丧的,，因为与此同时，其他的 CA 也可以为他们的域名颁发证书。

这种情况经常发生，但是以一种诚信的方式。当企业用户想要一个证书，不知道公司已经与某 CA 协商了预先存在的关系时，他会从他所选择的 CA 在线订购证书。不幸的是，证书可能是 CA 颁发给攻击者的。2011 年，在 Comodo 和 DigiNotar 都发生过这样的事情。在这两种情况下，攻击者找到了一种方法，可以让 CA 为域名颁发证书，即使域名所有者不是他们的客户。

许多行业专家一直在寻找方法，阻止 CA 为注册人未授权的域名颁发证书。解决这个问题的方法是证书颁发机构授权（CAA）。CAA 是在 RFC 6844 定义。

CAA 是一种 DNS 资源记录，它允许 DNS 域名持有者指定一个或多个授权的证书颁发机构为其域名颁发证书。这一规范有助于限制您对某一 CA 的信任,或者可以帮助你与你喜欢的 CA 协商数量折扣（价格优惠）。CAA 记录还可以为 CA 提供联系信息，允许 CA 通知域名所有者当他们收到一个不符合 CAA 记录偏好的请求。

CAA 资源记录的公开可以对公共 CA 实现额外的控制，以降低意外签发证书的风险。对 CA 的好处如下：

- 提高已验证域名的可靠性
- 降低将证书误发给具有较高网络钓鱼风险的域的机会
- 减少 CA 的攻击

尽管 CAA 的实施不是强制性的，但所有 CA 都有义务通过认证实践声明的证书政策（Certificate Policy of Certification Practice Statement）来公开他们的 CAA 政策。

请考虑使用 CAA 保护你的域名。

证书透明度(CT)

证书透明度（CT）是被提议的另一个方法，用来解决众多公共 CA 为任意域颁发 SSL 证书的问题。CT 目标如下：

- 使证书颁发机构不可能（或者至少是非常困难的）在颁发一个域名证书时，对其域名持有者却不可见。
- 尽可能保护用户免受错误颁发的证书的影响。

这是通过创建加密保证，公开审计，附加证书日志来实现的。每一个证书都将附有一个或多个日志的签名，用以声明该证书已经包含在这些日志中。浏览器、审计人员和监视器将协同工作以确保日志是可信的。域名所有者和其他相关方可以对误发的证书进行监视。

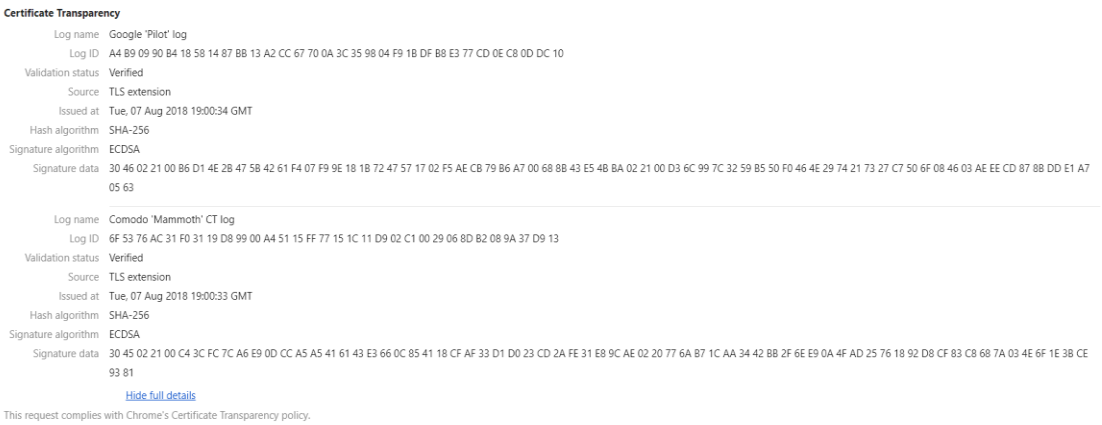
CT 的目标是在众多公开可用的日志中记录所有 SSL 证书。信任只会提供给已记录的证书。这些日志作为受信赖的对象是可审计的，并且还可以被监视以检测何时为任何特定的域名颁发了证书。

这对于 Internet 来说是一个巨大的好处，因为 CT 的解决方案适用于所有的域名以及所有的域名所有者，不管他们的网站大小或者站点的用途。域名所有者被允许监视日志，这可能是由第三方提供给他们的服务，比如大型搜索引擎公司或他们的 CA。

Chrome 将要求在 2018 年 4 月 30 日之后颁发的所有 TLS 服务器证书都符合 Chromium CT 政策，通过证书透明公开证书。如果证书在此日期之后发出，并且证书和站点都不支持 CT，那么这些证书将因不可信而被拒绝，并且连接将被

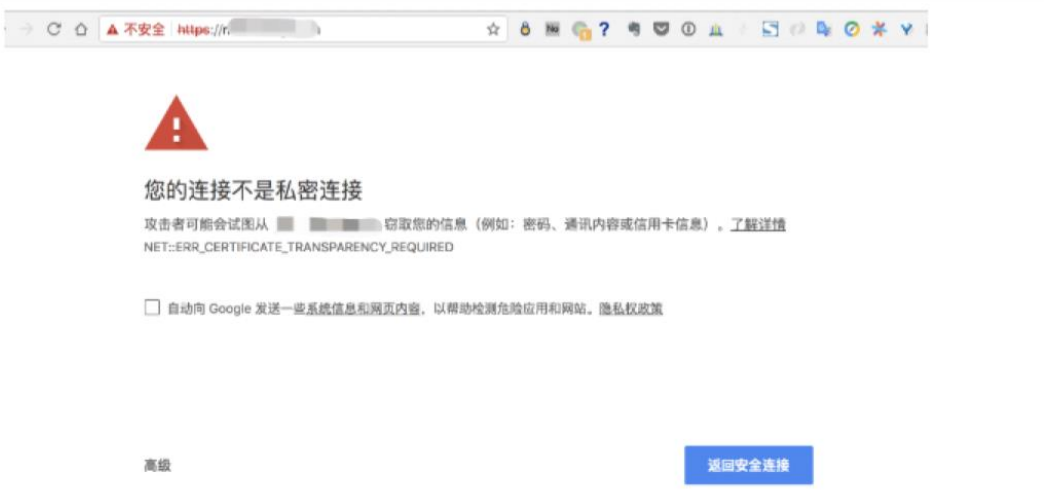
阻塞。在主页面加载的情况下，用户将看到一个完整的页面证书警告页面，并显示错误代码 net::ERR_CERTIFICATE_TRANSPARENCY_REQUIRED。如果您收到这个错误，这表明您的 CA 没有采取措施确保您的证书支持 CT，您应该联系您的 CA 销售或支持团队，以确保您能够获得一个有效的替代证书。

对于已记录的证书，例如在 Chrome 中，当您选择“透明信息”时，您将从每个日志中看到证书时间戳。



有了证书透明度，就可以监视日志，它记录了为给定域名颁发的所有证书。未经授权的证书会被处理掉和撤销。

Chrome 68 新的 CT 政策已实施，影响部分网站。新政策影响效果如下，外交部的邮件系统使用有效期为 2 年的 SSL 证书，其应该包含 3 个 SCT(已签证书时间戳，Signed Certificate Timestamp)，而该网站只有 2 个 SCT，故被 Chrome 68 拦截，Chrome 67 不受影响。



Lifetime of Certificate	Number of SCTs from distinct logs
< 15 months	2
>= 15, <= 27 months	3
> 27, <= 39 months	4
> 39 months	5

EV 证书的寿命不应大于 27 个月。

公钥固定（HTTP Public key pinning）

当前的浏览器-证书颁发机构（CA）信任模型允许网站所有者从任意一个 CA 中获得它的 SSL 证书。这种灵活性意味着由 CA 错误颁发的证书，即使该 CA 不是网站所有者选择的授权 CA，也会被浏览器视为可信赖的。

公钥固定或 HTTP 公钥固定（HPKP）允许网站所有者声明其 SSL 证书必须有一个或多个以下内容：

- 指定公钥
- 用此公钥进行 CA 签名
- 使用此公钥对 CA 进行等级信任

如果网站所有者的域名证书是由未列出的 CA 颁发的（例如不是固定的），支持 HPKP 的浏览器将提供信任对话警告。

注意：如果需要，网站所有者可以从多个 CA 中固定多个密钥，并且所有的密钥都将被浏览器视为有效。

网站所有者相信，它所选择的特定 CA 不会误发域名证书。这些 CA 通常限制谁可以请求为所有者指定的域颁发证书，这为防止未经授权的一方误发证书提供了额外的安全性。

正确的实施 HPKP 是一件很棘手的工作，因此，它主要是由一些高姿态、对安全性敏感的网站使用。如果您决定使用 HPKP，那么您应该从一个非常短的 max-age 值开始，如果没有任何问题再逐渐增加时长。

您可以通过 HPKP reporting 检测问题，最初是由 Chrome 46 提供的。

对于公钥固定报告。你可以尝试使用 Public-Key-Pins-Report-Only 头代替

Public-Key-Pins。 因为使用 Public-Key-Pins-Report-Only 头时，Chrome 只会验证 PIN 值是否匹配。而且一旦不匹配不会阻止你的连接，只会向你配置的报告地址发送一份报告。如果你只是尝试，你可以这么使用，不会对你的网站造成任何风险，而且还可以了解是否会给你的用户带来问题。

当您使用 Public-Key-Pins 头向浏览器传递 HTTP 公钥信息时，您也可以在该头中包含一个 report-uri 值，用于决定是否回报违反 HTTP 公钥固定策略的事例。

证书声誉

SSL 行业的优点之一是证书可以由最受信赖的 CA 颁发。这使得证书客户可以灵活地选择他们的 CA 或者决定使用哪些 CA。缺点是终端用户不知道颁发证书的 CA 是否被授权，而且证书可能具备欺诈性。

安全专家已经提出了允许域名所有者授权 CA（CAA，证书颁发机构授权）的建议，允许 Web 服务器声明可信的公钥（Public Key Pinning 公钥固定），或者允许网站所有者监控已经为其域名颁发的证书（CT，证书透明性）。

微软正在提出一种改进证书可信度的解决方案：证书声誉（Certificate Reputation）。在 Internet Explorer（IE）11 中，Microsoft 将扩展由 SmartScreen Filter 收集的遥测数据，以包含网站提供的 SSL 证书。他们将创建工具来构建由每个可信根 CA 颁发的所有证书的情报。

其目标是通过公开可信的证书标记潜在的中间人（MITM）攻击。已标记的例子有:

- 使用从属 CA 证书的网站。
- 网站为特定域提供不同的证书。
- 在 CA 颁发的证书领域发生重大变化，例如 OCSP 服务器位置。

证书声誉有以下优点：

- 隐私，当一个证书用户为其内部域名购买证书时，这个域名将不会公开。数据也会被加密发送，不会保留任何个人身份信息。
- 证书监控，当使用域名发布新证书时，可以通过电子邮件通知域名所有者。
- 可扩展，解决方案在不需要第三方（如网站运营商）合作的情况下可以

进行扩展。

- 部署，证书声誉（Certificate Reputation）易于部署，它只需要来自微软的努力。解决方案不依赖于诸如 CAs、订阅者、Web 服务器开发人员和 OCSP 开发人员等第三方执行的更改。

安全专家还说，存在着一些缺点：

- 没有公开日志，微软拥有该数据库，它不会公开发布，也无法用于审计。
- 敏感性，高度针对性的攻击将很难被发现。
- 未覆盖所有的证书，解决方案将依赖于使用 IE 11（及以后版本）收集的遥测数据。这意味着它针对的是浏览器而不是其他应用程序使用的证书。还有一个自愿退出的问题，一个组织可能不会向微软提供数据；这种情况下，这些网站将弃用该解决方案。

Google 支持 CT，对于 2018 年 4 月 30 日以后发布的所有新证书，Chrome 要求通过证书透明度公开证书。Microsoft 支持证书声誉提议，也支持证书透明度提议，并且从 2018 年 4 月 12 日起，颁发给 Microsoft 属性的所有证书都将包含 SCT 扩展。

网站所有者的一个担忧是，攻击者可以获得为其域名颁发的证书。

2015 年 3 月，微软部署了证书声誉。通过 Windows、Internet Explorer 和其他应用程序的使用，所有类型的 SSL 证书被收集并提供给了微软。微软没有收集任何可以用来识别用户身份的信息，因此，隐私可以得到维护。

证书数据只能由能够确认域名所有权的用户查看。这些数据由 Bing Webmaster Tools 提供，包含身份信息，比如服务器的名称、实体名称以及 CA 的名称，它还提供证书有效期和有效性的数据。它允许用户下载证书并向微软报告欺诈证书。

证书声誉的优点是它适用于所有类型的 SSL 证书，不仅仅是 EV。它适用于所有 CA，因为 CA 不需要参与到证书声誉计划。微软通过门户提供信息，所有管理员都可以使用证书声誉。缺点是它只提供来自 Windows 及其应用程序的数据。

注意：欺诈证书是一个日益严重的问题，因此建议域名所有者使用证书声誉来监视他们的域。

七、 高级证书

为了使企业的安全级别达到最高，有许多高级证书提供企业级别的安全保护。包括多 SAN 证书、扩展验证（EV）证书、椭圆曲线加密（ECC）证书和私人可信证书（Private Trust Certificates）。

多 SAN 证书

该证书有时称为统一通信证书（Unified Communications Certificate，UCC），多域名证书或多 SAN 证书。

UCC 证书的独特之处在于它充分利用了备用名称（SAN）字段，发行商允许证书用户在 SAN 字段中请求多个域名。

其结果是，UCC 提供了许多独特的优势：

- 灵活性，一个证书可以保护证书用户拥有的多个域和子域。支持在单个 IP 地址上通过 SSL 进行虚拟托管，并允许证书保护不止一个域名，比如 https://www.example.com 和 https://example.com。
- 兼容性，有些应用程序，如 Microsoft Exchange，需要保护的不止一个域名，也只需使用一个证书。
- 安全，UCC 证书只保护网站所有者指定的域名。该证书不保护攻击者设置的未知站点域名。与通配符证书比起来，这是一个很大的优势。
- 验证级别，UCC 可以使用域名验证（DV）、组织验证（OV）或最安全的扩展验证（EV）来发布。这允许网站所有者可以选择想要呈现给他们站点用户的验证级别。
- 价格效益，单个证书包含多个域名，其成本通常低于一个证书对应一个域名。

对于多 SAN 证书，优先排序最流行的域名，以减少浏览器连接时间。

多域 SSL 证书通过一个 SSL 证书来保护多个域、子域或主机名，与购买单

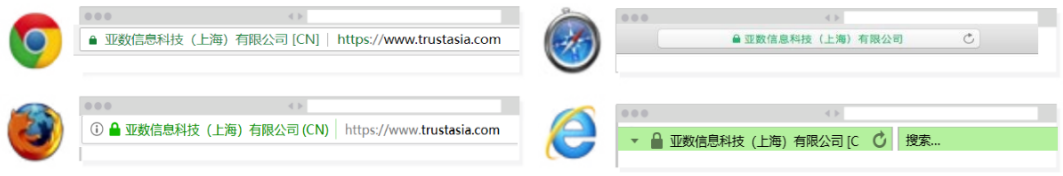
个证书相比，节省了您的时间和金钱。

扩展验证（EV）证书

在过去，浏览器和证书颁发机构（CA）没有 SSL 证书验证或管理的标准，这会导致在一些情况下，证书被错误地颁发。这使得诸如钓鱼网站之类的攻击获得了合法的证书。

CA 和 browsers 成立了 CA/Browser 论坛，并为扩展验证（EV）SSL 证书创建了标准。验证过程加强了所有者的身份识别，以及授权证书颁发。浏览器识别 EV SSL，状态栏显示为绿色。

多年来，遭受大量钓鱼攻击的网站已经转向 EV SSL。他们的顾客希望在绿色的状态栏里看到他们证书的信息。此信任可以扩展到所有者拥有的符合 EV 标准的网站。



专业提示：能够最高级别地确保网络安全。同时，这些证书充分利用了当今流行浏览器中添加的视觉提示——这是向你的客户表明你的网站是安全的一个明确的指示。

椭圆曲线加密（ECC）证书

椭圆曲线加密（ECC）是一种可以取代 RSA 或 DSA 的公钥加密算法。

ECC 与 RSA 加密算法相比，是一个完全不同的数学加密算法，使用的椭圆曲线是一个代数函数($y^2 = x^3 + ax + b$)。ECC 算法是单向的，易于计算，但是不可能反向计算以找到原始数据。

ECC 可用于椭圆曲线 DSA（ECDSA）数字签名，并在关键的交换中使用 Elliptic Curve Diffie-Hellman (ECDH)。数字证书可以使用 ECDSA 替代 RSA 签名。当服务器和客户端使用 ECDH 协商会话密钥时，ECC 也可以用于 SSL/TLS 握手。

ECC 的好处是，对于给定长度的密钥来说，ECC 密钥安全性更强。例如，256 位大小 ECC 密钥，相当于一个 3072 位的 RSA 密钥，比 2048 位 RSA 密钥

强大 1 万倍。这意味着随着 RSA 密钥越来越弱，我们可以转向使用 ECC 密钥，不再需要容纳更大的 RSA 密钥。在 SSL/TLS 握手过程使用 ECC，会比其他算法快得多，降低了站点的延迟，减轻服务器处理负担。此外，ECC 支持优先正向保密（PFS）。

ECC 的缺点是它不受所有客户端软件的支持。

如果您计划使用 ECC 证书，那么您可能需要一台服务器，它同时支持 RSA 密钥和 ECC 密钥。

私人可信证书（private trust certificates）

私人可信 SSL 证书允许使用当前拥有的未注册的域名，只要根证书也被分发，就可以使用这些域名。

该类证书的根证书会限定证书的域名，如下图所示：

```
X509v3 Name Constraints:
    Permitted:
      DNS:01.org
      DNS:acpica.org
      DNS:adsdcsp.com
      DNS:appup.com
      DNS:askintelsupport.com
      DNS:cilkplus.org
      DNS:clearlinux.org
      DNS:cloudinsights.com
      DNS:cloudnpo.org
      DNS:clusterconnection.com
      DNS:cofluentdesign.com
      DNS:crosswalk-project.org
      DNS:edacadtoolkit.org
      DNS:exascale-tech.com
      DNS:ibbprof.com
```

某根证书，在其扩展内约束了只能为这些域名颁发证书。一旦其颁发的证书域名不再该列表中，将被浏览器等拦截。

八、 可靠的证书颁发机构和 Always-On SSL：令人信任的组合

当涉及网站安全时，最好不要走捷径。你应该信任一个可靠的 CA 并部署 Always-On SSL。

值得信赖的 CA

一个可靠的 CA 会带给用户平和的心态和安全感，因为你知道你的网站正受到专业的保护。以下是可信 CA 的一些优点：

- CA 验证域名所有者和证书申请人
- CA 按照浏览器和操作系统供应商的要求制定政策。这些要求包括 CA/浏览器论坛基线需求（CA/Browser Forum Baseline Requirements）、扩展验证（EV）指南和 NIST 的建议。
- CA 提供质量保证。实施证书检查，确保不使用受损的密钥，遵循指导原则，确保使用的密钥不低于最小值，以及合理的散列算法、最大有效期和合理的证书扩展。
- CA 根据行业最佳实践更新政策
- CA 通过 CRL 和 OCSP 提供证书状态
- 被破坏的证书可以被撤销
- 根据证书发布标准对 CA 进行审核，标准如 WebTrust for CA、WebTrust for EV 和 SSL 基线要求
- 域名验证证书的证书请求者是由域所有者授权的。组织和扩展验证证书的请求者是由证书中指定的组织的成员授权的。
- CA 提供多种提醒，以确保证书在过期前被更新。CA 还提供证书发现工具，以便在您的系统上查找没有提醒的证书。

- CA 模型作为受大众信任的模型，主要是因为 CA 对于浏览器/OS 供应商，网站证书订阅者和网站最终用户是值得信任的第三方。CA 有义务满足所有三方的要求。

简而言之，尽管存在更便宜的选择，但没有一个像可靠的 CA 那样安全、可信和有效。最终，您预先节省的的几美元可能在将来的某个时候会因为完整数据的丢失而花费数千美元。

Always-On SSL

Always-On SSL 是一种保护你的网站以避免你的用户受到攻击的方法。Always-On SSL 涉及三个概念：全站 HTTPS，HTTPS 最佳实践以及带有领先技术的 SSL。

全站 HTTPS

Always-On SSL 可以避免你与你用户的会话被劫持。这意味着它不仅可以保护敏感的数据或金融交易，还对你的整个网站进行保护。我们的目标是确保您的用户使用 SSL 启动会话，并且永远不会关闭它，这有助于减轻常见工具的劫持攻击。

HTTPS 最佳实践

SSL 和它的实现一样强壮。通常，仅仅攻击不是一个聪明的黑客想要的结果，他想要的是一个简单的实现错误，可以让一个网站对攻击敞开了大门的错误。因为 SSL 部署在数千个不同的服务器/软件配置上，所以确保您的站点遵循最佳实践是保证网站完全性的关键。

下面是一些常见的配置小建议：

1. 始终确保您的 DNS 配置正确。这意味着将您的 www 和没有 www 的域地址指向同一个服务器。如果您的 www.example.com 地址指向一个服务器，而 example.com 指向另一个服务器或者根本没被解析，那么就会出现问题。

2. 在端口 80 和 443 上有不同的站点。考虑用相同的内容配置你的安全和不安全的网站。

3. 不要使用自签发证书。自签发证书会被浏览器拦截，一旦用户选择信任，那么即使真的出现问题时，也会被忽略。建议用信誉良好的公共 CA 颁发的证书替换自签名证书。

4. 确保正确配置 SSL 服务器。许多部署依赖于 Web 服务器的默认设置。不幸的是，这些默认设置可能是错误的或不安全的。使用 MySSL.com 来识别这些问题，然后适当的调整您的服务器。

5. 不要使用不完整的证书。用户输入网址并希望看到他想要的网站，但是却得到了一个证书错误提示。可以通过使用多域 SSL 证书来解决，该证书在备用名称（SAN）字段中既支持 example.com，也支持 www.example.com。

6. 不要在网站上混合 SSL 和纯文本。混合内容会导致中间人攻击。

7. SSL 不仅仅用于认证。使用 SSL 仅进行身份验证的站点很容易受到会话劫持的攻击。SSL 不仅用于身份验证，在会话的其余部分也将能用到 SSL。

8. 保证使用 Secure Cookie。不安全的 Cookie 会受到中间人攻击。

9. 保证使用安全的内容。使用混合的页面内容会损害安全性。一个纯文本链接就足以破坏整个安全的 SSL 站点。不要在页面上混合安全和不安全的内容。

具有领先技术的 SSL

如果您在整个站点上都有 SSL，通过减少不良实践可以确保安全性，那么您可以通过使用诸如以下的领先技术来升级您的安全性：

- EV SSL 证书
- HTTP 严格传输安全性（HSTS）
- OCSP 装订
- 优先正向保密（PFS）
- SHA-2 哈希
- TLS1.2

九、 工具

MySSL.com 服务器测试是很好的第一步，根据您的站点是如何构建来推荐配置和减少已知攻击。

下面是一些帮助您进行 SSL 部署的有用工具：

MySSL.com 是在线检测工具，对您部署的 HTTPS 网站进行综合检测，我们根据安全风险给出了 A+、A、A-、B、C、D、E、F、T 九个评级。

下图为 myssl.com 的评级报告：

漏洞检测工具帮助你检测你的网站可能存在的漏洞，包含：HeartBleed 检测、FREAK Attack 漏洞检测、SSL POODLE 漏洞检测、CCS 注入漏洞检测、CBC padding oracle 检测。

MySSL（https://myssl.com/）已经全方位的审查了 SSL/TLS 部署过程，提供了诸多工具，帮助您检测网站安全性，并希望为您提供最佳实践，使您可以在部署和维护上花费最少的时间，达到最佳的效果。

十、 攻击

一直以来，网站攻击越来越普遍，越来越复杂。一份全面的攻击清单需要几天的时间来阅读，在这里有一些近年来最常见、最臭名昭著的攻击。

BEAST(CVE-2011-3389)：Browser Exploit against SSL/TLS 的缩写，BEAST 针对 SSL 3.0 和 TLS 1.0 的 AES 加密实施所谓的选择性纯文本恢复攻击。AES 加密技术利用了一种称为密码块链接（CBC）的加密模式，在该模式中，来自前一个加密的数据块的数据用于对下一个数据块进行加密。

BEAST 攻击针对 TLS1.0 和更早版本的协议中的对称加密算法 CBC 模式，初始化向量 IV 可以预测，这就使得攻击者可以有效的讲 CBC 模式削弱为 ECB 模式，ECB 模式是不安全的。

CRIME(Compression Ratio Info-leak Made Easy CVE-2012-4929)：此攻击利用 SSL/TLS 的特性（SSL/TLS 用于实现 HTTPS），并影响 SSL 和 TLS 的所有版本。攻击是由需要加载到受害者浏览器上的代理执行的。攻击者还必须能够嗅探受害者的 HTTPS 流。

这是一种可攻击安全隐患，通过它可窃取启用数据压缩特性的 HTTPS 或 SPDY 协议传输的私密 Web Cookie。在成功读取身份验证 Cookie 后，攻击者可以实行会话劫持和发动进一步攻击。

FREAK(CVE-2015-0204)：FREAK 是中间人（MITM）漏洞，英文全称为“Factoring RSA-EXPORT Keys”.

客户端会在一个全安全强度的 RSA 握手过程中接受使用弱安全强度的出口 RSA 密钥，其中关键在于客户端并没有允许协商任何出口级别的 RSA 密码套件。

Heartbleed(心血漏洞 CVE-2014-0160) 是 OpenSSL 的程序漏洞，它允许攻击者通过 Internet 读取系统的内存，并危及私钥、姓名、密码和内容。采用“心血漏

洞”攻击不会被记录，所以它们是无法检测到的。攻击可以从客户端到服务器或服务器到客户端。如果使用带缺陷的 OpenSSL 版本，无论是服务器还是客户端，都可能因此受到攻击。此问题的原因是在实现 TLS 的心跳扩展时没有对输入进行适当的验证（缺少边界检查），该程序错误属于缓冲区过读，即可以读取的数据比应该允许读取的还多。

Logjam(CVE-2015-4000)：一个针对 Diffie-Hellman 密钥交换的安全漏洞，范围从 512 位（美国出口级）到 1024 位密钥。

使用 Diffie-Hellman 密钥交换协议的 TLS 连接很容易受到攻击，尤其是 DH 密钥中的公钥强度小于 1024bits。中间人攻击者可将有漏洞的 TLS 连接降级至使用 512 字节导出级加密。这种攻击会影响支持 DHE_EXPORT 密码的所有服务器。这个攻击可通过为两组弱 Diffie-Hellman 参数预先计算 512 字节质数完成，特别是 Apache 的 httpd 版本 2.1.5 到 2.4.7，以及 OpenSSL 的所有版本。

Lucky Thirteen：这个漏洞使用了一个已知的定时攻击，以前被认为是不切实际的。当使用（标准）CBC-mode 密码套件时，TLS 数据解密的工作方式有一个微妙的定时错误。在适当的情况下，攻击者可以使用这个来解密敏感信息，比如密码和 Cookies。

POODLE(贵宾犬漏洞 CVE-2014-3566)：贵宾犬攻击（Padding Oracle On Downgraded Legacy Encryption）允许从降级的通信中窃取如“安全”的 HTTP Cookie 或 HTTP Authorization 标头内容等项。贵宾犬漏洞的根本原因是 CBC 模式在设计上的缺陷，具体来说就是 CBC 只对明文进行了身份验证，但是没有对填充字节进行完整性校验。这使得攻击者可以对填充字节修改并且利用填充预示来恢复加密内容，让 POODLE 攻击成为可能的原因是 SSL3 中过于松散的填充结构和校验规则。

RC4 攻击：出自 RC4 对称加密算法的字节看起来并不是完全随机的，尽管它们有一些小的偏差。通过使用不同的密钥获取同一消息的不同的加密信息，攻击者可以利用这些小偏差发现加密的内容。

十一、 更新日志

日期	版本	版本修改信息
2018/09/05	V 1.0	第一版